PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2011/23

TrustyKey CA version 6.0.14

Paris, le 13 juillet 2011

Le directeur général de l'agence nationale
de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CC-2011/23**
Nom du produit **TrustyKey CA**
Référence/version du produit **Version 6.0.14**
Conformité à un profil de protection **Néant**
Critères d'évaluation et version **Critères Communs version 3.1 révision 2**
Niveau d'évaluation **EAL 3 augmenté** **ALC_FLR.3**
Développeur(s) **C.S.** **22 avenue Galilée, 92350 Le Plessis-Robinson, France**
Commanditaire **C.S.** **22 avenue Galilée, 92350 Le Plessis-Robinson, France**
Centre d'évaluation **Oppida** **4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France** **Tél : +33 (0)1 30 14 19 00, mél : cesti@oppida.fr**
Accords de reconnaissance applicables **CCRA** **SOG-IS**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est le logiciel « TrustyKey CA version 6.0.14 » développé par la société C.S.

Ce produit est destiné à être utilisé dans une infrastructure à clé publique (ICP, ou PKI pour *Public Key Infrastructure*). Une PKI est un ensemble de dispositifs matériels, de programmes logiciels et de procédures mis en œuvre par des personnes gérant notamment le cycle de vie des certificats. Ces certificats sont utilisés pour assurer des fonctions de sécurité telles que :

- l'authentification des utilisateurs ;
- le chiffrement de données ;
- la signature électronique ;
- la non-répudiation des transactions.

Le produit TrustyKey est une PKI flexible qui fournit des services opérationnels et d'administration pour gérer les certificats de tout type d'organisation. Il est composé principalement du composant TrustyKey CA (*Certification Autority*), qui gére les autorités de certification, reçoit et traite les demandes d'émission et de révocation de certificats, et publie le statut des certificats.

D'autres composants peuvent être déployés pour fournir des services supplémentaires :

- l'Autorité d'Enregistrement (AE), qui collecte les demandes de certificats pour les utilisateurs finaux, ainsi que la gestion des cartes pour les titulaires ;
- le Centre de pré initialisation (CPI), qui assure la pré-initialisation des tokens avec générations des clés de chiffrement en vue du séquestre ;
- le Centre de Recouvrement (CR), qui assure l'archivage sécurisé de clés privées de chiffrement, et permet le recouvrement en cas de perte de la clé.

Le déploiement de TrustyKey autorise la construction d'une ou plusieurs hiérarchies d'AC (autorité de certification). L'installation modulaire des serveurs de TrustyKey permet de s'adapter à la montée en charge du système.

La TOE (*Target of evaluation* – cible d'évaluation) est composée de l'autorité de certification de TrustyKey, dénommée par la suite TrustyKey CA.

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation. Elle s'inspire du niveau 2 du profil de protection « *Certificates Issuing and Management Components* » [PP CIMC].

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée de la TOE est identifiable :

- via le panneau de configuration, menu ajouter ou supprimer un programme : TrustyKey 6.0.14 ;
- via les barres de lancement d'applications : TrustyKey 6.0.14 ;
- via les fichiers .war du répertoire C:\CS\TrustyKeyCA\launcher\bin\webapps :
  - tkey-ca-web-6.0.19.war (pour TrustyKey CA Administration) ;
  - tkey-ca-ocsp-6.0.13.war (pour TrustyKey OCSP responder) ;
  - tkey-ca-cmp-6.0.15.war (pour TrustyKey CA Services) ;
- via l'interface web : TrustyKey CA 6.0.14.

La version du produit livré est disponible sur le bordereau de livraison accompagnant le produit.

L'intégrité du produit livré est vérifiable par comparaison des empreintes (SHA-256) générées par l'utilisateur, pour chaque fichier, avec celles disponibles sur le bordereau de livraison.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la génération et la signature de certificats ;
- la révocation de certificats ;
- la publication de listes de certificats révoqués ;
- la publication du statut de certificats ;
- l'identification et l'authentification des utilisateurs qui se connectent à l'autorité de certification ;
- la gestion des profils des utilisateurs en fonction des droits qui leur sont assignés ;
- le contrôle d'accès au système en fonction du profil de l'utilisateur ;
- la gestion des clés ;
- la gestion des journaux d'audit ;
- la protection des communications ;
- la sauvegarde et la restauration du système.

1.2.3. Architecture

Le produit TrustyKey CA comprend trois applications client-serveur :

- « TrustyKey CA services » : serveur de traitement de requêtes de demande de certificat et de révocation. Ces requêtes peuvent être fournies par l'autorité d'enregistrement ou par un CMP (*Card Management System* – système de gestion de cartes) ;
- « OCSP Responder » : serveur de traitement des requêtes OCSP (*Online certificate status protocol* – protocole de vérification en ligne de certificat). Ce serveur fournit l'état des certificats émis par l'autorité de certification ;
- « TrustyKey CA Administration » : serveur d'administration des services de l'autorité de certification à destination des opérateurs.

Le produit TrustyKey CA inclut des outils d'administration complémentaires locaux :

- une application d'initialisation qui permet la configuration et l'initialisation d'un serveur TrustyKey CA ;
- une application d'archivage et de restauration qui assure l'intégrité et la confidentialité des fichiers d'archive.

Les applications client-serveur de TrustyKey CA sont déployées sur des serveurs installés dans un domaine de confiance de l'infrastructure. Chacune de ces trois applications peut être installée sur plusieurs serveurs actifs pour assurer la montée en charge et la haute disponibilité. L'authentification forte des clients et la confidentialité des échanges sont assurées avec le protocole https sur le réseau.

La figure ci-dessous précise cette architecture :

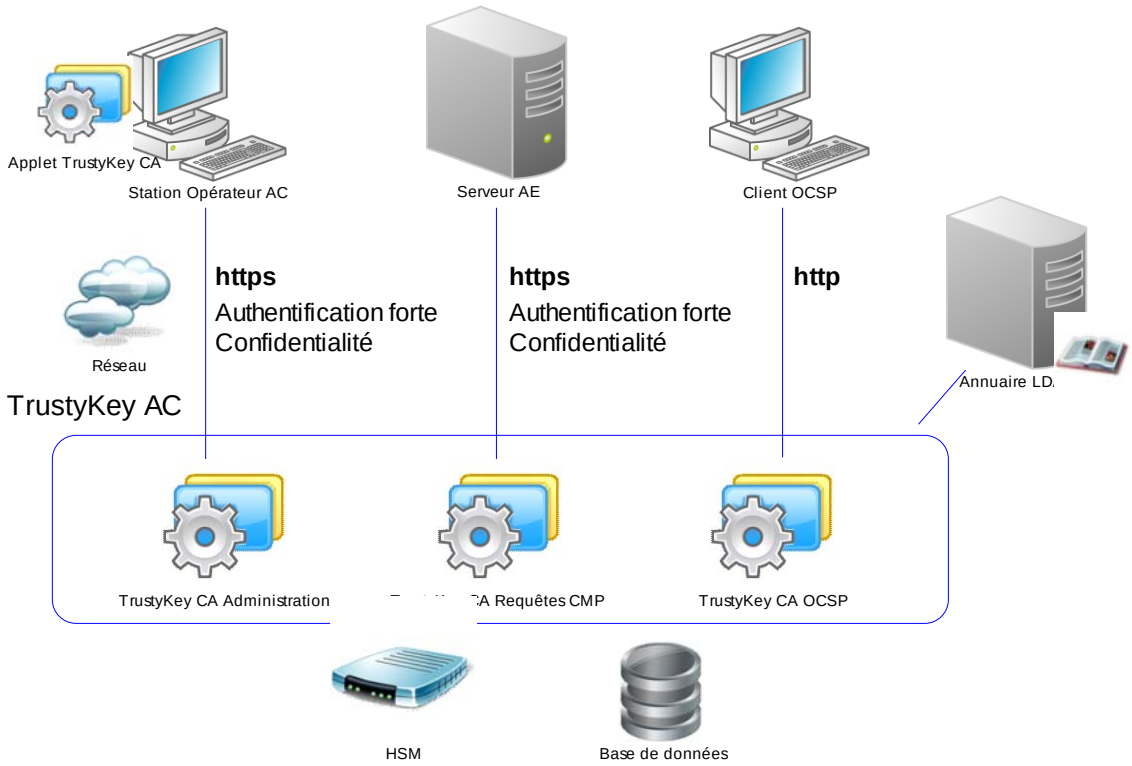

Figure 1 - Architecture de la TOE

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

- le développement et la livraison du produit sont réalisés par C.S. ;
- l'installation, l'administration et l'utilisation du produit correspondent au déploiement du produit par le client.

Le produit a été développé sur le site suivant :

C.S.

22 avenue Galilée
92350 Le Plessis-Robinson
France

Pour l'évaluation, l'évaluateur a considéré comme :

- administrateurs de la TOE les rôles suivants :
  - administrateur : son rôle est d'installer, de configurer et de maintenir la TOE ; d'assurer la gestion des comptes utilisateurs ; de configurer les profils des utilisateurs et les paramètres d'audit ; de générer les clés des composants du système ;
  - operateur : son rôle et de réaliser les sauvegardes et la restauration du système ;
  - auditeur : son rôle est de consulter et gérer les journaux d'audit ;
  - officier : son rôle est d'émettre des requêtes ou d'approuver des certificats ou des demandes de révocation de certificats ;
- utilisateurs de la TOE les rôles suivants :
  - autorité d'enregistrement : entité qui fait une demande d'émission ou de révocation de certificats ;
  - utilisateur final : utilisateur qui fait une demande relative au statut d'un certificat.

1.2.5. Configuration évaluée

La plateforme de tests mise en œuvre par le CESTI correspond à la configuration suivante :

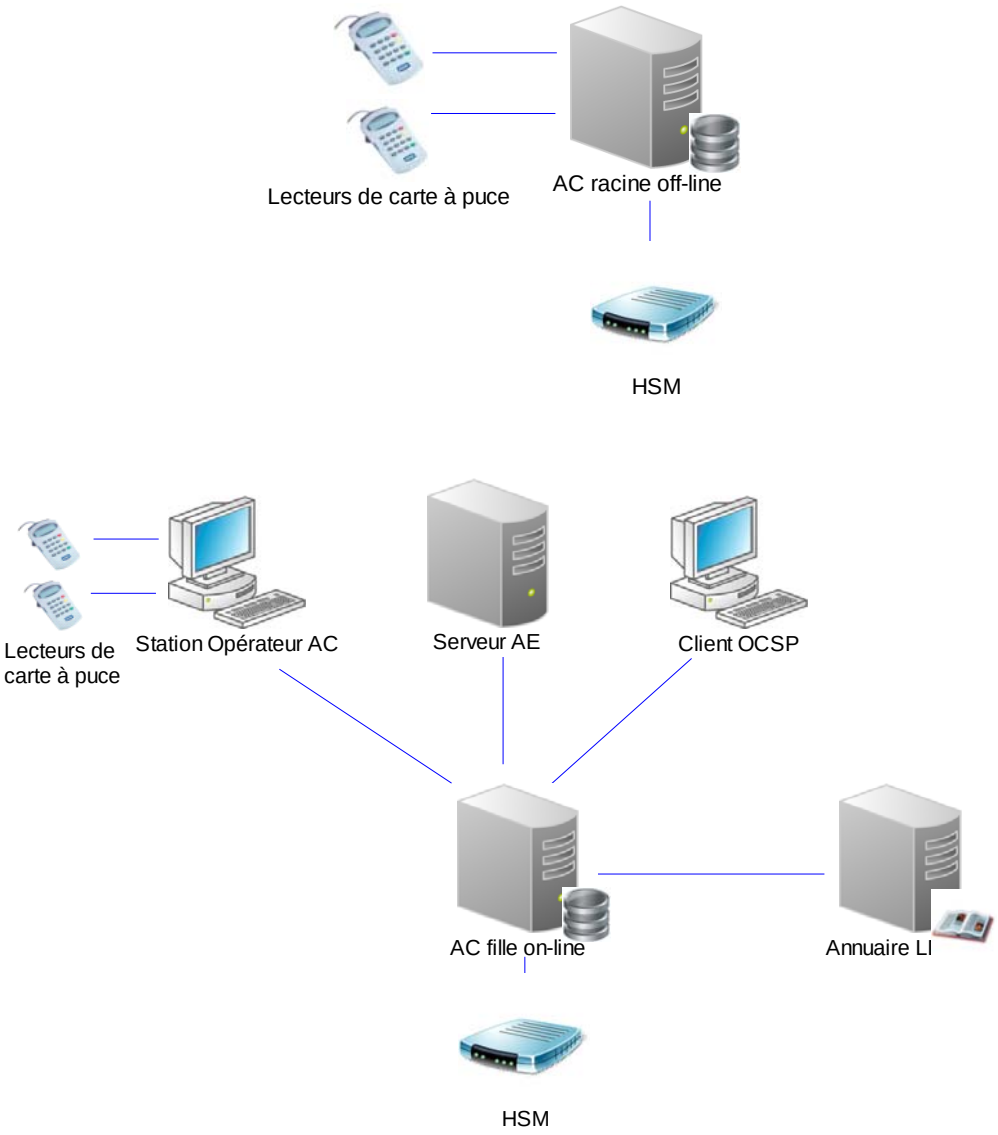

Figure 2 - Plateforme de tests

La plateforme de tests était constituée de deux TOE : une hors-ligne (AC racine), l'autre en ligne (AC fille).

La TOE hors-ligne était reliée à :

- deux lecteurs de cartes à puce ;
- un HSM (*Hardware Security Module* – Module matériel de sécurité) Safenet Luna CA4.

La TOE en ligne était reliée à :

- un client OCSP ;
- une station d'opérateur TrustyKey CA (elle-même reliée à 2 lecteurs de cartes à puce) ;
- un HSM Safenet Luna SA ;

- un annuaire LDAP (*Lightweight Directory Access Protocol* – Protocole d'accès aux annuaires léger) ;
- un serveur AE (permettant d'envoyer des requêtes de demande de génération et de révocation de certificat).

La plateforme d'évaluation est composée des équipements matériels et logiciels suivants :

- station opérateur :
  - système d'exploitation : Windows XP SP3 (32 bits) ;
  - Java : Java JRE 1.5.0.19 ;
  - navigateur : Internet Explorer 8 ;
  - lecteur de carte à puce : Omnikey Cardman 3821 ;
  - pilote du lecteur de carte à puce : Omnikey 1.1.2.4 ;
  - logiciel carte à puce : AuthentIC Web Pack 4.4 ;
- serveur AC racine :
  - système d'exploitation : Windows Server 2003 ;
  - Java : Java JRE 1.5.0.19 ;
  - base de données : Oracle 10g ;
  - HSM : Safenet Luna CA4 ;
  - navigateur : Internet Explorer 8 ;
  - lecteur de carte à puce : Omnikey Cardman 3821 ;
  - pilote du lecteur de carte à puce : Omnikey 1.1.2.4 ;
  - logiciel carte à puce : AuthentIC Web Pack 4.4 ;
- serveur AC :
  - système d'exploitation : Windows Server 2003 ;
  - Java : Java JRE 1.5.0.19 ;
  - base de données : Oracle 10g ;
  - HSM : Safenet Luna SA ;
  - navigateur : Internet Explorer 8 ;
  - lecteur de carte à puce : Omnikey Cardman 3821 ;
  - pilote du lecteur de carte à puce : Omnikey 1.1.2.4 ;
  - logiciel carte à puce : AuthentIC Web Pack 4.4 ;
- annuaire LDAP :
  - système d'exploitation : Fedora Core 9 ;
  - OpenLDAP 2.4 ;
- carte à puce :
  - AuthentIC ID-One Cosmo v5.4.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 2** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 7 juin 2011, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI [REF-CRY], [REF-KEY] et [REF-AUT] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le produit ne comporte pas de générateur d'aléas entrant dans le périmètre d'évaluation.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « TrustyKey CA, Version 6.0.14 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- identifier et surveiller les événements liés à la sécurité en faisant en sorte que les auditeurs lisent les journaux d'audit à une fréquence en rapport avec le niveau de risque (OE.Auditors Review Audit Logs) ;
- anticiper les possibles pertes d'évènements d'audit quand l'espace de stockage attribué aux journaux d'audit est plein, ou quasiment plein, en filtrant les évènements journalisés (OE.Respond to possible loss of stored audit records) ;
- s'assurer, à travers la mise en œuvre d'une gestion des données d'authentification, que les utilisateurs changent régulièrement et de façon appropriée leurs données d'authentification (note : cet objectif n'est pas applicable aux données d'authentification biométriques) (OE.Authentication Data Management) ;
- détruire de manière appropriée les données d'authentification et les privilèges associés après la suppression d'un accès (par exemple suite à une fin de contrat ou à un changement de responsabilité) (OE.Disposal of Authentication Data) ;
- assurer une protection physique des moyens de communication utilisés par la TOE (OE.Communications Protection) et des composants de la TOE (OE.Physical Protection) ;
- notifier aux autorités compétentes tous les problèmes de sécurité qui pourraient impacter leurs systèmes pour minimiser les risques de perte ou de compromission de données (OE.Notify Authorities of Security Issues) ;
- confier la gestion de la TOE et la sécurité des informations qu'elle contient à des administrateurs de la TOE compétents et de confiance (OE.Competent Administrators, Operator[CIMC]s, Officers and Auditors et OE.No Abusive Administrators, Operators, Officers and Auditors) ;
- rendre familières à tous les administrateurs de la TOE la politique de certification (PC) et la déclaration des pratiques de certification (DPC) sous lesquelles la TOE est exploitée (OE.CPS) ;

- délivrer aux utilisateurs et aux administrateurs de la TOE une formation aux techniques permettant de contrer les attaques par ingénierie sociale (OE.Social Engineering Training) ;
- s'assurer que les utilisateurs acceptent d'accomplir des tâches ou un groupe de tâches qui demandent un environnement des technologies de l'information sûr (OE.Cooperative Users) ;
- protéger la TOE de codes malveillants en s'assurant que tout code est signé par une autorité de confiance avant d'être chargé dans le système (OE.Malicious Code Not Signed)
- intégrer des mécanismes et des procédures pour prévenir des codes malveillants (OE.Prevent malicious code et OE.Procedures for preventing malicious code) ;
- effectuer des verifications périodiques d'intégrité, portant à la fois sur le système et sur les logiciels (OE.Periodically check integrity) ;
- fournir des jetons d'horodatage permettant de vérifier le bon séquencement des évènements (OE.Time stamps) ;
- maintenir à jour le système d'exploitation et la base de données en appliquant les patchs de sécurité.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 3+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**3**	Functional specification with complete summary
	ADV_IMP				**1**	1	**2**	2		
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**2**	Architectural design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**3**	Authorisation controls
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**3**	Implementation representation CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3		
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	**2**	**3**	3	**4**	**1**	Testing: basic design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**2**	Vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Security Target TrustyKey 6, Référence : CSSI/HLS/TRUSTY/ENG/08/0128, version 7.1 du 28 mars 2011, C.S.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation – Projet MORRIGAN, Référence : OPPIDA/CESTI/MORRIGAN/RTE, version 1 du 07 juin 2011, Oppida
[PP CIMC]	Certificate Issuing and Management Components – Family of Protection Profiles, version 1.0 du 31 octobre 2001. *Certifié par le NIST (National Institute of Standards and Technology) sous la référence CCEVS-VR-01-0009.*
[CONF]	Liste de configuration : - TrustyKey v6 – Configuration list, Référence : CSSI/HLS/TRUSTY/EN/10/0066, version 1.1 du 25 mai 2011, C.S.
[GUIDES]	Guide d'installation du produit : - TrustyKey 6 System guide for installation/deployment and administration, Référence : CSSI/HLS/TRUSTY/ENG/9/0053, version 1.1 du 2 décembre 2010, C.S. Guide d'administration du produit : - TrustyKey 6 CA – Administration Guide, Référence : CSSI/HLS/TRUSTY/ENG/8/0158, version 6.1 du 30 mars 2011, C.S. - Certificate generation profile creation guide, Référence : CSSI/HLS/TRUSTY/ENG/8/0137, version 1.1 du 2 novembre 2010, C.S. - Revocation list generation profile creation guide, Référence : CSSI/HLS/TRUSTY/ENG/8/0138, version 1.1 du 2 décembre 2010, C.S. Guide d'utilisation du produit : - TrustyKey 6 CA CMP and OCSP Interface guide, Référence : CSSI/HLS/TRUSTY/EN/10/0057, version 2.0 du 26 novembre 2010, C.S.

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr
[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr
[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr